IMPLEMENTASI WHIRLPOOL QR CODE PADA SISTEM KEAMANAN TRANSAKSI DIGITAL UNTUK MENJAGA INTEGRITAS DAN KEAMANAN DATA

SKRIPSI

Diajukan untuk memenuhi sebagian dari

Syarat Memperoleh Gelar Sarjana Komputer

Program Studi Ilmu Komputer

ICA NUR ANISA

1401527

PROGRAM STUDI ILMU KOMPUTER

DEPARTEMEN PENDIDIKAN ILMU KOMPUTER

FAKULTAS PENDIDIKAN MATEMATIKA DAN ILMU PENGETAHUAN ALAM

UNIVERSITAS PENDIDIKAN INDONESIA

2019

IMPLEMENTASI WHIRLPOOL QR CODE PADA SISTEM KEAMANAN TRANSAKSI DIGITAL UNTUK MENJAGA INTEGRITAS DAN KEAMANAN DATA

Oleh

Ica Nur Anisa

Sebuah skripsi yang diajukan untuk memenuhi salah satu syarat memperoleh gelar Sarjana pada Fakultas Pendidikan Matematika dan Ilmu Pengetahuan dan Alam

LEMBAR PENGESAHAN

IMPLEMENTASI WHIRLPOOL QR CODE PADA SISTEM KEAMANAN TRANSAKSI DIGITAL UNTUK MENJAGA INTEGRITAS DAN KEAMANAN DATA

Oleh

Ica Nur Anisa

1401527

Disetujui dan Disahkan oleh:
Pembimbing I

Rizki Rachman, JP., M.Kom
NIP. 197711252006041002

Pembimbing II

Harsa Wara P., M.Pd
NIP. 198008102009121003

Mengetahui,
Ketua Departemen Pendidikan Ilmu Komputer

Prof. Dr. H. Munir, M.IT.
NIP. 196603252001121001

IMPLEMENTASI WHIRLPOOL QR CODE
PADA SISTEM KEAMANAN TRANSAKSI DIGITAL UNTUK MENJAGA KEAMANAN INTEGRITAS DAN KEAMANAN DATA

Oleh
Ica Nur Anisa — ica.nuranisa@student.upi.edu
1401527

ABSTRAK

Sistem Keamanan Transaksi Digital merupakan aplikasi pembayaran transaksi digital yang memperkenalkan pada setiap proses transaksi yang dilakukan menggunakan *QR Code* sebagai pemindaian data atau bukti transaksi dan *fingerprint* sebagai akses untuk masuk/login ke aplikasi tersebut. Tujuan dibuatnya aplikasi *Sistem Keamanan Transaksi Digital* ini adalah mencegah adanya manipulasi data, menghemat waktu pembayaran, dan memudahkan pengguna untuk melakukan proses transaksi. Aplikasi ini berbasis android yang mengintegrasikan *fingerprint* sebagai *authentication* dalam proses transaksi. Pengguna disini akan memegang kendali aplikasi ini dan pengguna bisa mengetahui catatan atau hasil transaksi. Untuk proses pengujian tahapan ini dilakukan oleh pengguna secara langsung dan menghasilkan respon baik terhadap pengguna aplikasi tersebut, sehingga aplikasi yang dibuat termasuk dalam kategori baik dan cocok untuk membantu melakukan transaksi sehari-hari.

Kata kunci : *Fingerprint; QR Code;* Data Transaksi; Aplikasi Android

WHIRLPOOL QR CODE IMPLEMENTATION

ON DIGITAL TRANSACTION SECURITY SYSTEMS TO KEEP SECURITY INTEGRITY AND DATA SECURITY

Arranged by

Ica Nur Anisa — ica.nuranisa@student.upi.edu

1401527

ABSTRACT

Digital Transaction Security System is a digital transaction payment application that introduces each transaction process using the QR Code as a data scan or transaction proof and fingerprint as access to enter / login to the application. The purpose of making this *Digital Transaction Security System* application is to prevent data manipulation, save payment time, and make it easier for users to process transactions. This application is android based that integrates fingerprint as authentication in the transaction process. users here will take control of this application and users can find out the records or results of transactions. For the testing process this stage is carried out directly by the user and produces a good response to the user of the application, so that the application made is included in the good category and is suitable to help carry out daily transactions.

Keywords: Fingerprint; QR Code; Transaction Data; Android application

DAFTAR ISI

PERNYATAAN ..... **Error! Bookmark not defined.**
ABSTRAK 4
ABSTRACT 5
KATA PENGANTAR ..... **Error! Bookmark not defined.**
UCAPAN TERIMA KASIH ..... **Error! Bookmark not defined.**
DAFTAR ISI 6
DAFTAR TABEL 9
DAFTAR GAMBAR 10
BAB I PENDAHULUAN ..... **Error! Bookmark not defined.**
1.1 Latar Belakang ..... **Error! Bookmark not defined.**
1.2 Rumusan Masalah ..... **Error! Bookmark not defined.**
1.3 Tujuan ..... **Error! Bookmark not defined.**
1.4 Batasan Masalah ..... **Error! Bookmark not defined.**
1.5 Sistematika Penulisan ..... **Error! Bookmark not defined.**
BAB II KAJIAN TEORI ..... **Error! Bookmark not defined.**
2.1 Sistem Transaksi Digital ..... **Error! Bookmark not defined.**
2.2 Kriptografi ..... **Error! Bookmark not defined.**
2.2.1 Sejarah ..... **Error! Bookmark not defined.**
2.2.2 Tujuan Kriprografi ..... **Error! Bookmark not defined.**
2.2.3 Teknik Dasar Kriptografi ..... **Error! Bookmark not defined.**
2.2.4 Protokol Kriptografi ..... **Error! Bookmark not defined.**
2.2.5 Karakteristik Kriptografi ..... **Error! Bookmark not defined.**
2.3 Algoritma Whirlpool ..... **Error! Bookmark not defined.**
2.4 Fungsi *Hash* ..... **Error! Bookmark not defined.**
2.5 QR Code (Quick Response Code) ..... **Error! Bookmark not defined.**
2.6 Representasi Citra Digital ..... **Error! Bookmark not defined.**
2.7 Base 64 ..... **Error! Bookmark not defined.**

2.8 Fingerprint..... **Error! Bookmark not defined.**

2.9 *One Time Password*..... **Error! Bookmark not defined.**

2.10 *Man-In-The-Middle-Attact*..... **Error! Bookmark not defined.**

BAB III METODOLOGI PENELITIAN..... **Error! Bookmark not defined.**

3.1 Desain Penelitian..... **Error! Bookmark not defined.**

3.2 Alat dan Bahan Penelitian..... **Error! Bookmark not defined.**

3.2.1 Alat Penelitian..... **Error! Bookmark not defined.**

3.2.2 Bahan Penelitian..... **Error! Bookmark not defined.**

3.3 Metode Penelitian..... **Error! Bookmark not defined.**

3.3.1 Pengumpulan Data ..... **Error! Bookmark not defined.**

3.3.2 Pengembangan Perangkat Lunak Error! Bookmark not defined.

BAB IV PENELITIAN DAN PEMBAHASAN ... **Error! Bookmark not defined.**

4.1 Hasil Penelitian ..... **Error! Bookmark not defined.**

4.2 Algoritma Whirlpool ..... **Error! Bookmark not defined.**

4.2.1 Penguatan Merkle-Damgard..... **Error! Bookmark not defined.**

4.2.2 S-box Whirlpool ..... **Error! Bookmark not defined.**

4.3 Proses verifikasi fingerprint..... **Error! Bookmark not defined.**

4.4. Proses Transaksi..... **Error! Bookmark not defined.**

4.4.1 Alur Implementasi QR Code..... **Error! Bookmark not defined.**

4.4.2 Proses Verifikasi Kode OTP ..... **Error! Bookmark not defined.**

4.4.3 Proses hasil implementasi fungsi hash..... **Error! Bookmark not defined.**

4.5 Pengembangan perangkat lunak..... **Error! Bookmark not defined.**

4.5.1 Deskripsi sistem ..... **Error! Bookmark not defined.**

4.5.2 Batasan Perangkat Lunak..... **Error! Bookmark not defined.**

4.5.3 Proses operasional perangkat lunak ..... **Error! Bookmark not defined.**

4.5.4 Perancangan..... **Error! Bookmark not defined.**

4.5.5 Implementasi..... **Error! Bookmark not defined.**

4.6 Pengujian ..... **Error! Bookmark not defined.**

4.7 Pembahasan implementasi whirlpool pada sistem transaksi digital... **Error! Bookmark not defined.**

4.7.1 Hasil hash ..... **Error! Bookmark not defined.**

4.7.2 S-box Whirlpool ..... **Error! Bookmark not defined.**

4.7.3 Merkle-damgard ..... **Error! Bookmark not defined.**

4.8 Implementasi whirlpool ke dalam sistem transaksi digital ..... **Error! Bookmark not defined.**

4.9 Memodifikasi transaksi digital ..... **Error! Bookmark not defined.**

4.10 Hasil Implementasi QR Code pada sistem transaksi digital ..... **Error! Bookmark not defined.**

4.11 Pengujian sistem dengan *Man-in-the-Middle-Attack***Error! Bookmark not defined.**

4.12 Hasil Pengujian Man-in-the-Middle-Attact**Error! Bookmark not defined.**

4.13 Hasil Pembahasan whirlpool qr code pada sistem transaksi digital... **Error! Bookmark not defined.**

BAB V..... **Error! Bookmark not defined.**

KESIMPULAN DAN SARAN ..... **Error! Bookmark not defined.**

5.1 Kesimpulan ..... **Error! Bookmark not defined.**

5.2 Saran ..... **Error! Bookmark not defined.**

DAFTAR PUSTAKA 12

DAFTAR TABEL

Tabel 4. 1 Isi dari mini-box E..... **Error! Bookmark not defined.**
Tabel 4. 2 Isi dari mini-box E^{-1} ..... **Error! Bookmark not defined.**
Tabel 4. 3 Isi dari mini-box R ..... **Error! Bookmark not defined.**
Tabel 4. 4 Block Message ..... **Error! Bookmark not defined.**
Tabel 4. 5 Padding bits pengganjal "1" dan "0".... **Error! Bookmark not defined.**
Tabel 4. 6 S-box Whirlpool..... **Error! Bookmark not defined.**
Tabel 4. 7 Mini box E(u)..... **Error! Bookmark not defined.**
Tabel 4. 8 Mini box E^{-1}(u) invers dari E..... **Error! Bookmark not defined.**
Tabel 4. 9 Mini box R(u) acak semu ..... **Error! Bookmark not defined.**
Tabel 4. 10 Modul Program ..... **Error! Bookmark not defined.**
Tabel 4. 11 Modul program library ..... **Error! Bookmark not defined.**
Tabel 4. 12 Pengujian menggunakan metode black box..... **Error! Bookmark not defined.**
Tabel 4. 13 Block message dan string ..... **Error! Bookmark not defined.**
Tabel 4. 14 Perbandingan hasil hash..... **Error! Bookmark not defined.**
Tabel 4. 15 Block message whirlpool..... **Error! Bookmark not defined.**
Tabel 4. 16 *Hash Computed*..... **Error! Bookmark not defined.**
Tabel 4. 17 Hasil Pengujian Man-in-the-Middle-Attact..... **Error! Bookmark not defined.**
Tabel 4. 18 Hasil uji implementasi..... **Error! Bookmark not defined.**

DAFTAR GAMBAR

Gambar 2. 1 Enkripsi dan Deskripsi (Nugraha, Pasca, & Munir, 2011) ..... **Error! Bookmark not defined.**

Gambar 2. 2 Skema Merkle-Damgard (Gunawan, 2007) .... **Error! Bookmark not defined.**

Gambar 2. 3 Skema hash dengan Miyaguchi-Preenel (Gunawan, 2007) ..... **Error! Bookmark not defined.**

Gambar 2. 4 Aliran Data Whirlpool (Nugraha, Pasca, & Munir, 2011)..... **Error! Bookmark not defined.**

Gambar 2. 5 Struktur Rekursif S-box ..... **Error! Bookmark not defined.**

Gambar 2. 6 Fungsi hash menghasilkan fingerprint (Stallings, 2014). ..... **Error! Bookmark not defined.**

Gambar 2. 7 QR Code (Covic & Simon, 2016) .... **Error! Bookmark not defined.**

Gambar 2. 8 Proses Pembangkitan QR Code (Ardhianto & Wahyudi, 2012) ..... **Error! Bookmark not defined.**

Gambar 2. 9 Proses Pembacan QR Code (Ardhianto & Wahyudi, 2012) .... **Error! Bookmark not defined.**

Gambar 2. 10 Struktur *QR Code* (Muharom, 2016). ..... **Error! Bookmark not defined.**

Gambar 2. 11 Citra Digital Matriks (Nugraha, Pasca, & Munir, 2011) ..... **Error! Bookmark not defined.**

Gambar 2. 12 Arsitektur Fingerprint (Pradana, Ifan, & Hari, 2013) ..... **Error! Bookmark not defined.**

Gambar 2. 13 Pola Sidik jari (Umamaheswaril, et al., 2007)..... **Error! Bookmark not defined.**

Gambar 2. 14 Metode *Optical Scanning*..... **Error! Bookmark not defined.**

Gambar 3. 1 Desain Penelitian.....**Error! Bookmark not defined.**
Gambar 3. 2 Model Modern Watefall (Sommerville, 2011)**Error! Bookmark not defined.**
Gambar 4. 1 Alur proses implementasi fingerprint.....32
Gambar 4. 1 Alur proses implementasi fingerprint**Error! Bookmark not defined.**
Gambar 4. 2 Alur Convert Image Base64 *Fingeprint* ..... **Error! Bookmark not defined.**
Gambar 4. 3 Alur Proses Hash Image *Fingerprint* **Error! Bookmark not defined.**
Gambar 4. 4 Alur proses implementasi QR Code . **Error! Bookmark not defined.**
Gambar 4. 5 Convert File Csv ke JSON ..... **Error! Bookmark not defined.**
Gambar 4. 6 Alur Proses Hash data String JSON . **Error! Bookmark not defined.**
Gambar 4. 7 Proses Generate Hasil hash ke QR Code ..... **Error! Bookmark not defined.**
Gambar 4. 8 Alur Verifikasi Kode OTP ..... **Error! Bookmark not defined.**
Gambar 4. 9 Alur implementasi fungsi hash..... **Error! Bookmark not defined.**
Gambar 4. 10 Perancangan *Use Case Diagram* .... **Error! Bookmark not defined.**
Gambar 4. 11 Antarmuka desktop ..... **Error! Bookmark not defined.**
Gambar 4. 12 Tampilan Awal Aplikasi ..... **Error! Bookmark not defined.**
Gambar 4. 13 Scan fingerprint ..... **Error! Bookmark not defined.**
Gambar 4. 14 Informasi saldo ..... **Error! Bookmark not defined.**
Gambar 4. 15 Scan Qr code..... **Error! Bookmark not defined.**
Gambar 4. 16 Rincian Transaksi ..... **Error! Bookmark not defined.**
Gambar 4. 17 Transaksi Sukses..... **Error! Bookmark not defined.**
Gambar 4. 18 Kode Verifikasi..... **Error! Bookmark not defined.**
Gambar 4. 19 Proses Implementasi Fingerprint .... **Error! Bookmark not defined.**
Gambar 4. 20 Proses Implementasi Data CSV..... **Error! Bookmark not defined.**
Gambar 4. 21 Sistem Modifikasi Transaksi Digital ..... **Error! Bookmark not defined.**
Gambar 4. 22 Hasil Implementasi QR Code..... **Error! Bookmark not defined.**

Gambar 4. 23 Pengujian alur proses sistem keseluruhan..... **Error! Bookmark not defined.**
Gambar 4. 24 Pengujian tahap I terjadinya serangan man-in-the-middle-attact ..... **Error! Bookmark not defined.**
Gambar 4. 25 Pengujian tahap II terjadinya serangan tampering pada sistem ..... **Error! Bookmark not defined.**
Gambar 4. 26 Pengujian implementasi whirlpool Man-in-the-Middle-attack**Error! Bookmark not defined.**

DAFTAR PUSTAKA

Aldrin, N. (2017). Analysis of Product Buying Decision on Lazada E-commerce based on Previous Buyers' Comments. *Evropejskij Issledovatel'*, *2*(8), 70–77.

Ani, N., Deby, R., Nugraha, M. P., & Munir, R. (2011). Pengembangan Aplikasi QR Code Generator dan QR Code Reader dari Data Berbentuk Image. *Konferensi Nasional Informatika – KNIF 2011*, 148–155. https://doi.org/10.1016/S0887-8994(99)00149-6

Anshori, H, M., Samopa, F., & Suryotrisongko, H. (2013). Pengembangan sistem pembayaran elektronik menggunakan kode qr berbasis android. *Jurnal Teknik Pomits*, *2*(1), 2–4.

Aryasa, K., & Paulus, Y. T. (2013). Implementasi Secure Hash Algorithm-1 Untuk Pengamanan Data Dalam Library Pada Pemrograman Java. *Creative Information Technology Journal*, *1*(1), 57–66.

Dey, S. K., Uddin, M. R., Kabir, K. M., & Rahman, M. M. (2017). Enhancing the security of cloud computing: Genetic algorithm and QR code approach. In *Advances in Electrical Engineering (ICAEE), 2017 4th International Conference on* (pp. 181–186).

Ghosh, B. S., Goswami, J., Majumder, A., Kumar, A., & Mohanty, S. P. (2017). Swing-Pay: A Digital Card Module using NFC and Biometric Authentication for Peer-to-Peer Payment. *IEEE Consumer Electronics Magazine*, *6*(1), 1–15.

Gunawan, A. (2006). Studi Mengenai Algoritma Simetri, 1–18.

IFAN, P. H. (2015). Klasifikasi Citra Sidik Jari Berdasarkan Enam Tipe Pattern Menggunakan Metode Euclidean Distance. *Skripsi*, *Fakultas Ilmu Komputer*.

Joshi, M. R., & Karkade, R. A. (2015). Network security with cryptography. *IJCSMC*, *4*(1), 201–204.

Khairnar, S., & Kharat, R. (2016). Survey on secure online voting system. *Int. J. of Comput. Appl*, *134*(13), 19–21.

Kitsos, P., & Koufopavlou, O. (2004). Efficient architecture and hardware implementation of the whirlpool hash function. *IEEE Transactions on Consumer Electronics*, *50*(1), 208–213. https://doi.org/10.1109/TCE.2004.1277864

Lee, S.-J., Lee, J. S., Lee, M.-K., Lee, S. J., Choi, D.-H., & Kim, D. K. (2011). Low-Power Design of Hardware One-Time Password Generators for Card-Type OTPs. *ETRI Journal*, *33*(4), 611–620.

Mallik, A., Ahsan, A., Shahadat, M. M. Z., & Tsou, J.-C. (2019). Man-in-the-middle-attack: Understanding in simple words. *International Journal of Data and Network Science*, *3*, 77–92. https://doi.org/10.5267/j.ijdns.2019.1.001

Mittra, P., & Rakesh, N. (2017). A desktop application of QR code for data security and authentication. *Proceedings of the International Conference on Inventive Computation Technologies, ICICT 2016*, *2*. https://doi.org/10.1109/INVENTIVE.2016.7824809

Nor, R. M., Ali, N. A. M., Azmi, K., Marzuki, A., Nor, L. M., & Yusof, M. (2017). ScanMed: A mobile medicine adherence application with intake validation using QR code. *Proceedings - 6th International Conference on Information and Communication Technology for the Muslim World, ICT4M 2016*, 112–117. https://doi.org/10.1109/ICT4M.2016.29

Perry, M., & Ferreira, J. (2018). Moneywork: Practices of Use and Social Interaction around Digital and Analog Money. *ACM Transactions on Computer-Human Interaction (TOCHI)*, *24*(6), 41. https://doi.org/10.1145/3162082

Putra, I. M. E. W., Dantes, G. R., & Candiasa, I. M. (2018). Model Pengukuran Tingkat Kepercayaan Pelanggan (Online Trust) Terhadap Situs E-Commerce (Studi Kasus pada Pelanggan E-Commerce di Provinsi Bali). *International Journal of Natural Science and Engineering*, *1*(3), 100–109. Retrieved from https://ejournal.undiksha.ac.id/index.php/IJNSE/article/view/12939

Rennie, S. J., Marcheret, E., Mroueh, Y., Ross, J., & Goel, V. (2017). Self-critical sequence training for image captioning. In *Proceedings of the IEEE Conference on Computer Vision and Pattern Recognition* (pp. 7008–7024).

Sherlyanita, A. K., & Rakhmawati, N. A. (2016). Pengaruh dan Pola Aktivitas Penggunaan Internet serta Media Sosial pada Siswa SMPN 52 Surabaya. *Journal of Information Systems Engineering and Business Intelligence*, *2*(1), 17. https://doi.org/10.20473/jisebi.2.1.17-22

Umamaheswari, K., Sumathi, S., Sivanandam, S. N., & Anburajan, K. K. N. (2007). Efficient finger print image classification and recognition using neural network data mining. *Proceedings of ICSCN 2007: International Conference on Signal Processing Communications and Networking*, 426–432. https://doi.org/10.1109/ICSCN.2007.350775

Yuricha, Y., Tursina, T., & Nasution, H. (2017). Implementasi Algoritma Kriptografi XXTEA untuk Enkripsi dan Dekripsi Query Database pada Aplikasi Online Test (Studi Kasus: SMK Immanuel Pontianak). *Jurnal Sistem Dan Teknologi Informasi (JustIN)*, *5*(1), 42–46.